Security and Privacy Aspects of Embodied AI and Robotics

Julya Rebstock & John Caras

BROADCOM

Agenda

- Introduction
- Key Terms
- Embodied AI Interactions
- Security Aspects of Embodied AI
- Privacy Aspects of Embodied AI
- Safety, Trust and Risks of Embodied AI
- Identifying Gaps in ITU-T Recommendations
- Real World Cases for Embodied AI

Study Group 21 Scope

Mandate: Study Group 21 focuses on multimedia technologies, systems, applications, and services for current and future networks, including IP-based and cable-based networks. This includes ICTs for multimedia systems and services, accessibility for digital inclusion, active assisted living, human interfaces, multimedia aspects of distributed ledger technologies (DLTs), media and signal coding, and digital multimedia services for various verticals such as digital health, digital culture, and mobility. It also covers multimedia aspects of metaverse-related issues.

Key Responsibilities: The group is responsible for the use of telecommunication systems for the contribution, primary and secondary distribution of audiovisual content, and immersive multimedia applications like virtual reality, augmented reality, and 3D. It also oversees the use of telecommunication networks, including coaxial cable, optical fibre, hybrid fibre-coaxial cable, and IP networks, to provide integrated broadband services. Additionally, the group leverages advanced technologies such as cloud computing and AI to enhance multimedia applications and services.

Study Group 17 Scope

ITU-T Study Group 17 (SG17) focuses on cybersecurity, security management, and protection of ICTs and the data they transmit. It's mandate includes developing standards for cloud computing, big data, and applications like social networks, all of which involve data protection.

Areas of Study:

- Security model, framework, architecture and lifecycle
- Cybersecurity and service
- Security Management
- End-device, edge, network, cloud and application security
- Data protection techniques
- New and emerging security technologies
- Open system interconnection (OSI) and technical languages
- Identity management and telebiometrics architecture and mechanisms

AI Definitions - SG17 - Draft CG-AISEC-STRAT-O-13-R1 "Artificial Intelligence Security Standardization Strategy"

- **3.2.1 Artificial intelligence (AI)**: capability of an engineered system to acquire, process, and apply knowledge and skills to achieve defined objectives.
- **3.2.21 Agentic artificial intelligence (agentic AI)**: An engineered AI system capable of autonomously pursuing human-defined objectives by planning, reasoning, and executing tasks across dynamic environments.
- **3.2.3 Embodied Artificial Intelligence:** An AI system integrated into a physical entity enabling perception, reasoning, and action within the physical environment.
- **3.2.4 Disembodied Artificial Intelligence**: An AI system that operates entirely in software without a physical embodiment or direct interaction with the physical environment, functioning through digital interfaces such as text, voice, or data exchange.
- **3.2.5 Embedded Artificial Intelligence**: AI functionality that is integrated directly into a device, system, or component, enabling local processing of data and autonomous decision-making, without reliance on external computing resources.
- **Appendix II** - Key focus areas of AI security standardization within SG17

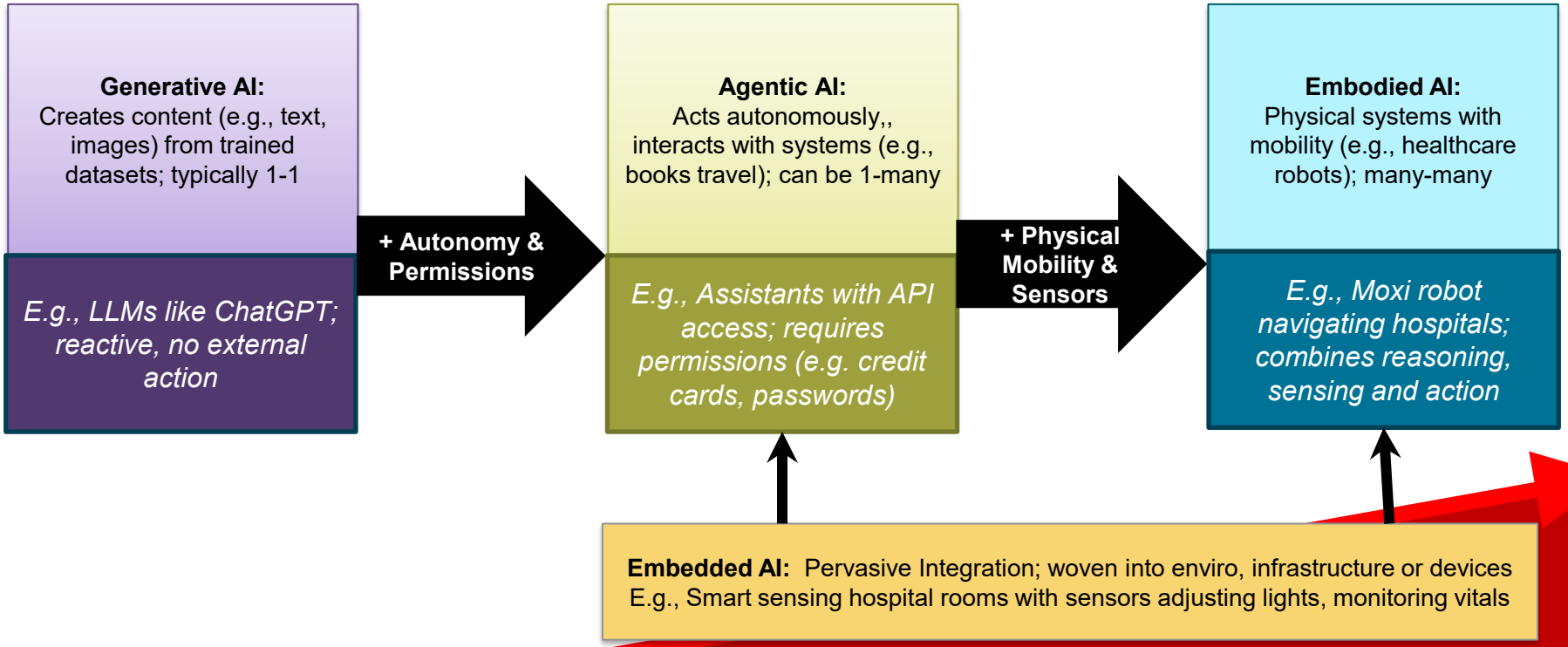
BROADCOM

AI Strategy for SG17: Draft CG-AISEC-STRAT-O-13-R1

- **Appendix II - Key focus areas of AI security standardization within SG17**
  - Security architecture and lifecycle protection for AI systems
  - Secure use of AI for enhancing ICT security
  - Security of AI systems and applications
  - AI in identity management and biometrics
  - AI security in vertical ICT applications
  - AI-driven data protection and privacy
  - Enterprise AI Governance, evaluation, and standardization roadmaps
  - Emerging AI-related threats and countermeasures
  - Interoperability and ecosystem coordination for AI security

BROADCOM

AI Progression: From Generative to Embodied & Embedded



Embodied AI Interaction: How do I determine what is human?

3 – Laws of Robotics

REGULATING HUMAN AUTONOMOUS INTERACTION

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.

1. A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.

1. A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

— Isaac Asimov

BROADCOM

Levels of Telebiometric Quantification

Organized by Complexity

- Biological Properties
- Determine Biological Species
- Identify Unique Action
- Prioritize Secure Interaction

Level 1: Application detects biological properties.

Level 2: Application determines which species.

Level 3: Application determines unique actions of each biological entity.

Level 4: Application prioritizes secure interactions with the biological entities.

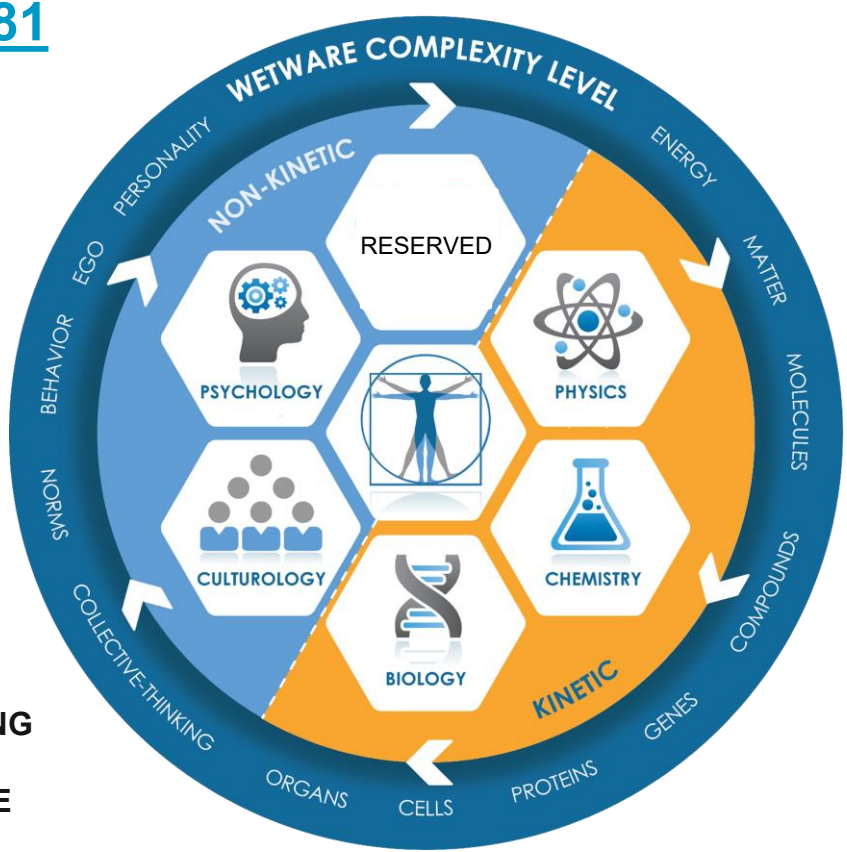
BROADCOM

Telebiometric Multimodal Model Interaction Model

ITU-T: SG17 X.1081

PSYCHOLOGICAL DOMAIN
- MEMES
- SYMBOLS
- MEMORIES
- ASSOCIATIONS
- INTELLIGENCE
- EMOTION

CULTURAL DOMAIN
- ETHNICITY
- CITIZENSHIP
- STATE
- CITY
- RELIGION
- COLLECTIVE THINKING
- NORMS
- POLITICAL DOCTRINE



Telebiometrics. Inc © 2025

PHYSICS DOMAIN
- HEAT
- RADIATION
- SOUND
- ELECTRICITY
- MAGNETISM
- LIGHT
- MASS

CHEMICAL DOMAIN
- OXYGEN
- WATER
- BLOOD CHEMISTRY
- URINE CHEMISTRY
- FOOD
- SUPPLEMENTS
- MEDICINE

BIOLOGICAL DOMAIN
- ANATOMY
- PHYSIOLOGY
- FUNCTION
- DISTRIBUTION

BROADCOM

From Interaction to Biology to Machine Protocol (B2M)

ITU-T: X.1080.2

B2M = (Interaction + Biosignal + Communication)

Purpose:

- To extend the Internet of Things (IoT) to include biological endpoints with a universal language.

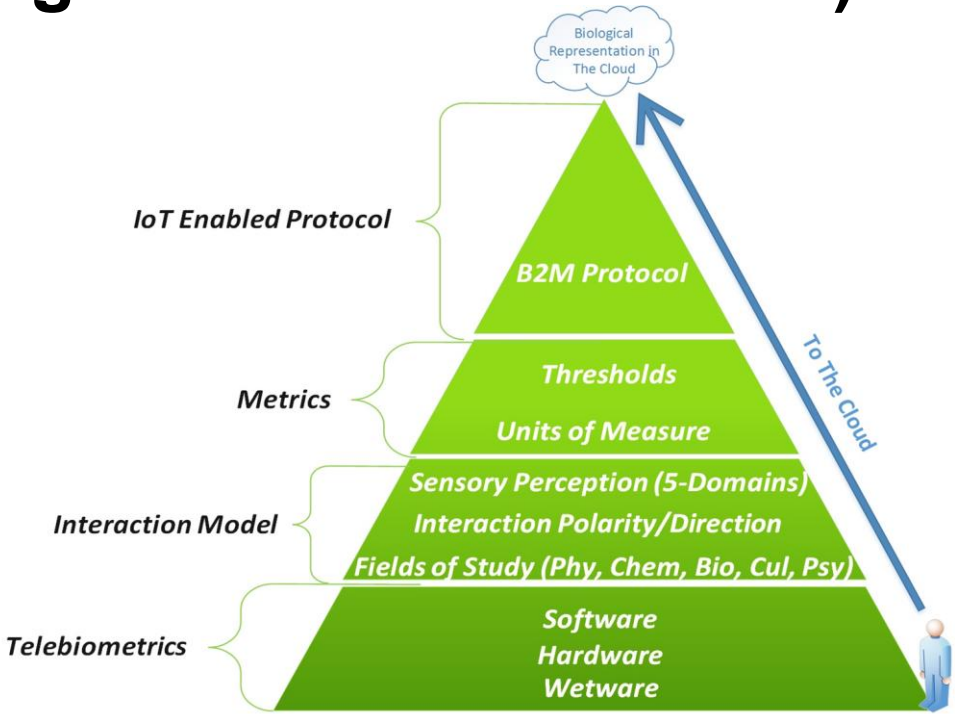
Mission:

- To organize biological information and make it universally accessible and useful.

Goal:

- To make B2M a native protocol to IoT devices globally.

"The human body is the next computer interface."
— David Navarro



Telebiometrics. Inc © 2025

BROADCOM

Core Security Risks - DATA

- **Data Risks in Model-to-Model Communications:**
  - **Leakage**
    - Sensitive information exposure
    - Prompt injection propagation
  - **Integrity & Authenticity**
    - Unverified trust chains
    - No source attribution
  - **Transmission**
    - In-transit exposure
    - Reply or man-in-the-middle attacks
  - **Context Contamination**
    - Cascade risks
    - Amplification

BROADCOM

Core Security Risks - PRIVACY

- **Unauthorized Collection**
  - Overcollection
  - Hidden in training data
- **Data leakage**
  - Prompt injection
  - Cross-context exposure
  - 3rd party sharing
- **Function Creep**
  - Re-purposing without consent
  - Insufficient anonymization
- **Regulatory Misalignment**
  - PII – GDPR, CCPA/CPRA, Brazil LGPD, Mexico ARCO, China PIPL, India DPDP, Japan APPI, South Korea PIPA, South Africa POPIA, etc.
  - PCI – storing or transmitting PCI data insecurely is a major violation
  - Training vs. Storage – if data is used for model weights you can't remove it without retraining or fine-tuning; unlike logs or databases
  - NO CURRENT ADHERENCE

BROADCOM

Global Privacy Regulations w/Erasure - Correction Rights

Correction Rights are nearly universal; erasure rights are increasingly standard but sometimes limited:

- **EU**: GDPR; UK GDPR & Data Protection Act
- **Americas**: HIPAA; CCPA/CPRA (California); Brazil LGPD; Mexico Federal Law on Protection of Personal Data; Canada PIPEDA
- **Asia-Pacific**: China PIPL; India DPDP Act; Japan APPI; South Korea PIPA; Australia Privacy Act
- **Middle East & Africa**: UAE Data Protection Law; Qatar Data Protection Law; South Africa POPIA; Kenya Data Protection Act

BROADCOM

Core Security Risks – SAFETY & TRUST

- **Component Dependency**
  - Sensors
  - Actuators/arms/bodies
  - Embedded software/firmware
- **Firmware/Driver Backdoors**
- **Updating Supply Chains**
  - OTA updates for components
- **Cascade Risk**
  - Liability ambiguity - how to you pinpoint a failure (sensor manufacturer, operator or supplier?)
- **Trust Escalation** – each stage requires more permissions

BROADCOM

Risk Amplifiers in Multi-Model Systems

- **Generative AI:** Model learns and cites sensitive data
- **Agentic AI**: Model takes autonomous action, but a corrupted communication could lead to unauthorized tasks
- **Embodied AI**: Data miscommunication between navigation, perception and control; capturing **biometrics** or conversations via sensors/mics/cameras (GDPR Article 9 Special Category)
- **Embedded AI:** Continuous monitoring and communications across infrastructure increases system vulnerability

BROADCOM

Risk Amplifiers – Embodied AI

- Embodied AI **trusts sensor inputs** to navigate and act
  - Poisoned sensors □ potential physical consequences
- Robotics has **tight feedback loops** — milliseconds between perception and action.
  - Limited time to detect and filter bad data.
- Supply chains are global, complex, and fragmented
  - Provenance harder
  - Updates fragmented

BROADCOM

Mitigation Strategies

- Data Minimization + Differential Privacy + Synthetic data
- Consent & Transparency
- Supplier Vetting & Assurance, Contracts, Liability
- Secure Firmware & Hardware
- System Architecture, Defense in depth
- Cryptographic Controls
- Provenance Tagging
- Access controls, Isolation, Mediation
- Continuous Monitoring and Logging
- Red-teaming and Adversarial testing

Where can ITU fill the gaps or extend for SECURITY?

- Inter-model communication security
- Machine unlearning/selective deletion/”right to be forgotten”
- Supply chain/Component trust
- Privacy by design & data governance mandates
- Auditability, traceability, provenance metadata
- Assurance levels & certification

BROADCOM

Where can ITU fill the gaps or extend for BIOLOGICAL?

Current AI Standards don't Recognize Life as Autonomous Systems:

1. **Missing Life recognition protocols** into AI interoperability frameworks. The prevailing AI standards landscape is predominantly machine-to-machine or machine-to-data in orientation. Users are conceptualized as data subjects, endpoints, or stakeholders, but not as autonomous biological systems that continuously adapt, respond, and require protection.
2. **Absence of Biological Metrics:** Without incorporating biosignals (e.g., ITU-T X.1094) and life indicators into standards, AI cannot reliably distinguish or prioritize living systems in critical interactions.
3. **Security Misalignment: Data Protection vs. Life Protection:** Most AI standards equate "protection" with data privacy and cybersecurity safeguards. This is necessary but insufficient.
4. **Ignoring Interaction Complexity:** Life forms are dynamic, adaptive, and complex systems that interact (ITU-T X.1080.2, ITU-T X.1081) within their environment. Standards for AI Embodied Systems interacting with biological systems is underdeveloped.

BROADCOM

EXAMPLES: AI USE IN MULTIMEDIA

USE CASE: AI in Google Home Devices

Gemini for Home is Google's next-gen AI assistant built on its large language models, meant to replace the more rule-based parts of Google Assistant in smart home contexts. It adds more conversational, context-aware interactions, letting you issue more natural and complex commands to control devices, search camera footage, or build automations.

Feature	What it Does
AI Descriptions for Camera Events	Instead of generic alerts like "motion detected" or "person seen," Gemini can generate a short or longer description (e.g. "dog digging in the garden") to give more context.
Search Camera History via Natural Language	You can ask things like "Was the FedEx truck here today?" or "Did the kids play in the backyard this afternoon?" rather than scrubbing through all clips manually. Gemini helps find relevant video segments.
"Help Me Create" / Natural Language Automation Building	Rather than configuring automations via UI menus, you can "tell Gemini what you want" (e.g. "turn on lights at sunset, but not in the guest room") and it drafts or suggests a routine.

BROADCOM

Telehealth = Telebiometrics + Telemedicine

It's all about the data……

- Telehealth - is the use of electronic information and telecommunications technologies to support long-distance clinical health care, patient and professional health-related education, public health and health administration.
- Telebiometrics – remote monitoring and reporting of biometric data.
- Telemedicine - the remote diagnosis and treatment of patients by means of telecommunications technology.
- Professor Enrico M. Staderini MD, PhD of Western Switzerland University of Applied Sciences discussed a quantified decision process for medical therapy from "*Handbook of analytic philosophy of medicine*" by Kazem Sadegh-Zadeh, Springer 2012.
- **Diagnosis in Medical treatment especially in Telemedicine is very dependent upon the quality of biological measurements.**

Healthcare Application: Baby Monitor

Reducing Sudden Infant Death Syndrome (SIDS)

Telebiometrics

e-Health

Baby monitor measures:

- Heart Rate (beats per minute)
- Body Temperature (C°/F°)
- Oxygen Saturation (%)

The monitor consists of a base station and a wristband with 3-sensors tuned to wetware thresholds for heart rate, temperature, and oxygen saturation quantification.

The user sets alert ranges for each of the measurements. The wristband quantifies the biological target and transmits a message back to the base station. When the baby “Life Signs” fall out of range and alert is enabled.

Alerts parents to the possibility of Sudden Infant Death Syndrome (SIDS)!

BROADCOM

Healthcare Application: Occupancy

Home Health Activity Monitor for Assisted Living

Ambient Assisted Living

In elderly care situations, a single senior citizen lives alone. Telebiometric motion sensors designed specifically for radiation emissions from a human body are placed throughout the house.

When a patient ceases to move an alarm or phone can ring to check on patient's status.

Adjustable sensitivity allows for detection in sleep.

BROADCOM

Embodied AI: Medical Robots

- Surgical
- Exoskeleton
- Rehabilitation
- Social

Moxi - sensors, cameras, AI; non-patient facing tasks

Robot Nurse Bear - capable of lifting/moving patients

Robot Paro - conversation, entertainment programs, comfort/affection

BROADCOM

Appendix/Reference

Thoughts to Ponder - Biometrics Privacy

How do you secure the privacy of all bystanders? Even if the robot/embodied device is not directly interacting with "you" but you are in the vicinity, the sensors would automatically be detecting and cataloging your presence. The device is going to uniquely identify me based on my biometric signature (i.e., facial recognition, capillaries in my face, physical characteristics of how the machine identifies me as a human, etc.).

- Where is this information logged, stored, transmitted, etc.? Since its likely a connected device, is it using Wifi, Bluetooth, NFC? What about data sovereignty?
- Who has access to this information? What RBAC exist to guarantee the integrity of my Biometric PHI (capillary definition, heart rate, etc. are all classified as PHI)
- How would you classify my presence? Just as "background noise" but not a direct interaction? Is there a "range" of how far away from the AI device the other bio-entities are detected/recorded?
- How long would my detected presence be retained?
- Privacy implications fall under multiple existing regulations:
  - **EU AI Act**, Article 5, 6, 8-15, 26
  - **GDPR**, Article 4, 9, 22 - processing personal data such as facial recognition requires DPIA, consent and data minimization; sensors can lead to unauthorized data collection
  - **United States**:
    - FTC 28 CFR Part 202
    - Illinois Biometric Information Privacy Act; Texas Capture or Use Of Biometric Identifier Act; Washington Biometric Privacy Protection Act (also wraps in health data); California CPRA; Colorado Privacy Act; Virginia CDPA; Connecticut CTDPA
  - **China** PIPL, Articles 13, 25, 28, 51, 55; China Cybersecurity Law and Measure for the Security Management of Facial Recognition Technology, Articles 4, 5, 7, 9, 12, 21
  - **Canada** Quebec IT Act, Section 44; Canada PIPEDA
  - **New Zealand** Draft Biometrics Code
  - **Australia** Privacy Act

BROADCOM

Thoughts to Ponder - Biometrics Legal

What would be the legal controls on harm caused by an AI device? In general, embodied AI, due to its physical interactions and potential applications (healthcare robots, autonomous vehicles, industrial automation) triggers high-stakes risks.

- **EU AI Act**: defines AI into four tiers:
  - Unacceptable Risk - includes biometric surveillance by law enforcement (i.e., robot police dogs?)
  - High Risk - includes embodied AI like autonomous vehicles, safety components/sensors
  - Limited risk - AI generated content
  - Minimal risk.
  - complements revisions to the Product Liability Directive that was updated to cover AI-enabled products and a proposed AI Liability Directive (currently withdrawn)
- **US** - No federal AI law but Tort and product liability laws would treat AI harms like defective products and manufacturers can be held liable for design flaws or failures
- **US National Highway Traffic Safety Admin** has issued guidelines for autonomous vehicles, and more specifics in California, Arizona, Georgia, and Colorado
- **UK** has an Automated Vehicles Act
- **UNESCO** Recommendations on the Ethics of AI requires AI respects human rights, prevents harm and promotes accountability.
- **World Health Org** guidelines for AI in health emphasize ethical deployment to avoid harm
- So far, the few cases where harm was caused have fallen to producers of the software or physical devices.
- Black-box type requirements seems most common to log how/why actions were taken

Thoughts to Ponder - Biometrics Compliance

GRC is *significantly* impacted by the deployment of embodied AI as these systems introduce unique risks such as physical harm, sensor failures, or even unpredictable behavior. GRC frameworks emphasize governance, risk management and compliance.

- **EU AI Act** - embodied AI fall under High Risk categories due to potential physical harms, property damage or societal impact (think what would happen if a robot shows bias towards a certain race while performing its duties); these systems would have to be registered in the EU database, certify conformity, maintain event logs for auditing, and maintain transparency obligations which if we don't even understand what its actually doing or how... we cant document transparency or provide reasonable reporting. Also have to document and ensure the entire supply chain (i.e., sensor manufacturers) meet any standards.
- **US NHTSA**/ Federal Automated Vehicles Policy - must submit safety assessments for autonomous vehicles, sensor reliability, cybersecurity and crash avoidance plus yearly safety updates
- **US FDA** - for medical embodied AI, surgical systems etc, falls under 21 CFR Part 820, requires validating AI algorithms, ensuring sensor accuracy and reporting adverse events in the Medical Device Reporting system
- **US OSHA** for Workplace robots - industrial robots must copy with 29 CFR 1910 to prevent worker injuries from AI
- ***US States have over 100 bills introduced in 2025 so far***
- **UK** Automated Vehicles Act - self driving requirements for safety records, sensor reliability, reporting incidents
- **China** AI Regs - embodied AI has mandated safety certifications for drones and robots under the Cybersecurity Law
- **ISO** 13482:2014 (Robots and Robotic Devices)
- **ISO** 26262 (Automotive Functional Safety)
- **ISO/IEC** 42001 (AI Management Systems)
- **IEEE** 7000 servers (i.e., IEEE P7001 for transparency)
- **NIST** Cybersecurity Framework (CSF 2.0) has risk assessment for sensor vulnerabilities and incident response plans
- **EU** Cybersecurity Act and NIS2 Directive - both require AI in critical infrastructure (logistics robots) meet cybersecurity certifications and have reporting requirements within 24 hours
- **UNESCO** Recommendations on the Ethics of AI - requires risk assessments for physical safety and human rights to ensure no discrimination or harm (biased sensor data causing accidents)

BROADCOM

Asimov's Laws vs. Modern AI Standards

Asimov's Law	Modern AI Standards	Remaining Gaps
First Law **No harm to humans**	• UNESCO AI Ethics: dignity & safety • OECD: robustness & safety • ISO/IEC & IEEE: risk management	• No life recognition • Biosignals not included • Only risk reduction, not prohibition
Second Law **Obey human orders**	• Human-in-the-loop oversight • ITU/ISO accountability frameworks	• Cannot verify real human identity • Cannot filter malicious orders
Third Law **Self-preservation**	• Reliability & robustness standards • Cybersecurity frameworks (ISO/IEC 27000)	• Survival not life-centric • Systems may resist shutdown • Focus on uptime, not ethics
Zeroth Law **No harm to humanity**	• UNESCO & UN SDGs: collective wellbeing • IEEE 7010: wellbeing metrics • UNEP/ITU AI & climate	• No technical enforcement • Trade-offs between individual & collective • Ecosystem protection underdeveloped

BROADCOM

THANK YOU!

Julya Rebstock, CIPT
julya.rebstock@broadcom.com
Enterprise Security Group - Symantec - Broadcom
https://www.linkedin.com/in/julya-rebstock/

John Caras
408.387.4700
John.Caras@Telebiometrics.com
www.telebiometrics.com
https://www.linkedin.com/in/johncaras/